BRENNUS 4.0

LETTRE D'INFORMATION DU CENTRE DE DOCTRINE ET D'ENSEIGNEMENT DU COMMANDEMENT

N° 7 – MARS 2020

SOMMAIRE

- Cyber, cyber… Vous avez dit cyber ?
- Les origines historiques de la guerre électronique
- Les enjeux du cyber pour l'armée de Terre
- La cyberdéfense est d'abord un combat
- La conquête des ressources humaines en cyberdéfense
- La stratégie française de cyberdéfense
- L'organisation de la cyberdéfense au sein de l'OTAN
- La conduite des opérations cyber
- Les systèmes d'information, l'intelligence artificielle et le cyber
- Les câbles sous-marins entre vulnérabilité et enjeu stratégique

LES ENGAGEMENTS DANS LE CYBERESPACE

Une nouvelle étape pour la cyberdéfense de l'armée de Terre

L'armée de Terre a créé sa première section de lutte informatique défensive en 2000. L'année 2019 a ouvert une nouvelle étape. En effet, dans le cyberespace, les armées ont longtemps été cantonnées à des actions défensives. En janvier 2019, les déclarations de la Ministre des Armées au FIC (Forum International de la Cybersécurité) 2019 suivies par la publication d'une doctrine militaire de lutte informatique offensive marquent la volonté d'engager les armées sur l'ensemble des missions, « renseigner-défendre-agir ».

Le cyberespace fait partie intégrante de notre vie quotidienne comme de nos opérations. Pour l'armée de Terre, il s'agit de continuer à s'approprier la cyberdéfense avec pragmatisme et volontarisme, en liaison avec le COMCYBER. L'exploitation des possibilités offertes permettra d'accroître l'efficacité opérationnelle de nos unités.

Avec les combats menés dans l'environnement informationnel et dans l'environnement électromagnétique, les engagements dans le cyberespace rentrent dans la catégorie des actions dans les champs immatériels. L'importance de ces actions pour nos combats de demain avait été identifiée dans « Action Terrestre Future ». Elle a déjà été confirmée en Ukraine, au Levant, et, de plus en plus, en Afrique.

La cyberdéfense n'est plus un sujet réservé à quelques spécialistes. L'ensemble de nos états-majors opérationnels doit s'approprier ce nouveau domaine de lutte afin d'être capable d'intégrer les effets dans le cyberespace à la manœuvre interarmes, tant en planification qu'en conduite. Ces effets pourront être produits par des moyens de l'armée de Terre, mais le plus souvent, par des capacités du COMCYBER.

Dans la perspective de nos engagements en haute intensité, comprendre les principes, le rôle des acteurs et les enjeux de la cyberdéfense est fondamental. Ce numéro de Brennus contribue à cette nécessaire appropriation.

Bonne lecture !

Général de division Patrick Brethous, sous-chef opérations-aéroterrestres de l'armée de Terre (SCOAT)

CE DOCUMENT DE REFLEXION N'ENGAGE PAS L'ÉTAT-MAJOR DE L'ARMEE DE TERRE

Directeur de la publication : général de division Michel DELION - CDEC - 1, place Joffre - Case 53 - 75700 PARIS SP 07 - Secrétariat 01 44 42 51 02 - Fax secrétariat 01 44 42 81 29 • **Rédacteur en chef :** colonel Fabrice CLÉE, 01 44 42 38 93 • **Secrétaires de rédaction :** chef de bataillon ® Guillaume LASCONJARIAS, lieutenant-colonel Georges HOUSSET, chef de bataillon Olivier TILLIER, Monsieur Jean-Philippe GIRAUD • **Éditeur rédactionnel :** chef de bataillon Olivier TILLIER • **Maquette :** chef de bataillon Olivier TILLIER/CDEC/PEP • **Impression - Routage :** EDIACA - 76, rue de la Talaudière - CS 80508 - 42007 SAINT-ÉTIENNE Cedex 1 - 04 77 95 33 21 ou 04 77 95 33 25 • **Tirage :** 506 exemplaires • **Diffusion :** CDEC/DAD/PUB - 01 44 42 43 18 • **Dépôt légal :** Avril 2019 - **ISSN :** 2650-703X - **ISBN imprimeur :** 978-2-11-155119-0 - **ISBN numérique :** 978-2-11-155120-6 • La version électronique de ce document est en ligne sur les sites internet : **cdec.terre.defense.gouv.fr** et **https://www.penseemiliterre.fr/** •

Tous droits de reproduction du document sont soumis à l'autorisation préalable de la rédaction.

Les articles complets sont accessibles sur le site www.penseemiliterre.fr ou directement sur les liens indiqués dans chaque brève.

LES ENGAGEMENTS DANS LE CYBERESPACE

Cyber, cyber...vous avez dit cyber ?, par le colonel Jean-Michel Fouquet, commandant l'enseignement militaire supérieur scientifique et technique du CDEC

Cybernétique, cyberdéfense, cyberattaque, cyberprotection, cybersécurité : autant de termes utilisant le préfixe cyber. Ce préfixe qui « sert à former de nombreux mots relatifs à l'utilisation du réseau Internet » est pourtant trop souvent utilisé seul, sans qu'aucune adjonction n'y soit associée pour constituer un mot dérivé à la signification bien précise. Cette utilisation abusive est génératrice de nombreuses interrogations, voire d'incompréhensions et nuit à l'appropriation de termes pourtant clairs et intelligibles. Aussi convient-il de faire l'effort nécessaire pour être précis dans les termes employés afin que « les mots nous arrivent aisément » et que l'action se conçoive avec une claire vision de l'esprit de la mission.

De la même manière qu'un spécialiste en mécanique définit son référentiel d'étude avant d'aborder et résoudre un problème, la précision dans les termes relevant du domaine cybernétique sera gage d'une meilleure compréhension par l'ensemble des acteurs de la cyberdéfense, et donc d'une efficacité renforcée dans les actions dans le cyberespace, notamment dans le cadre de la mise en œuvre de la stratégie française de cyberdéfense.

Intraterre : EN SAVOIR + **Internet : EN SAVOIR +**

Les origines historiques de la guerre électronique, par le lieutenant-colonel Georges Housset, du pôle études et prospective du CDEC

Quel intérêt peut-il y avoir à se pencher, à l'heure de l'infovalorisation et du cyber, sur des temps reculés, dans lesquels la science et les techniques en sont à leurs balbutiements ? Est-ce la menace brandie par un Thucydide d'une « histoire qui n'est qu'un éternel recommencement » ou la vision prospective d'un Einstein qui a prétendu en son temps : « je ne sais pas quelles seront les armes de la prochaine guerre mondiale, mais celles de la suivante seront des haches de pierre », qui peuvent justifier l'intérêt d'un coup d'œil dans le rétroviseur ?

Étant donné qu'un des objectifs des forces terrestres est de préparer la guerre de demain, il apparaît en tous cas légitime de s'interroger sur ce que pourraient être les *modus operandi* du conflit à venir. Après avoir eu la guerre des chimistes (Première Guerre mondiale), parce que le gaz moutarde et le chlore y ont été employés pour la première fois, puis la guerre des physiciens (Deuxième Guerre mondiale), en raison de l'éclosion de la bombe atomique, dans quelle mesure un conflit à venir ne pourrait-il pas consacrer les mathématiciens ? En effet, selon les spécialistes de l'art de la guerre, un des enjeux militaires du futur pourrait consister à pénétrer à l'intérieur du commandement ennemi et, le prenant de vitesse, avoir la capacité d'anticiper ses décisions tactiques.

Intraterre : EN SAVOIR + **Internet : EN SAVOIR +**

Les enjeux du cyberespace pour l'armée de Terre, par le lieutenant-colonel Julien Cheize de la division doctrine du CDEC

Les forces terrestres se modernisent sous l'impulsion de la réforme « Au Contact » et le début du déploiement du programme SCORPION. Elles vont disposer dans les mois et les années à venir de matériels majeurs extrêmement modernes, qu'il s'agisse de véhicules, de Sytèmes d'Armes (SA) ou de Systèmes d'Information Opérationnels et de Communication (SIOC). Cela a entraîné une réflexion de fond globale sur la conduite des opérations, entre rupture et continuité, avec un certain nombre de nouvelles opportunités offertes par ces nouvelles capacités. En parallèle de cette mutation majeure des forces terrestres, d'autres enjeux ont été identifiés afin d'être anticipés dès à présent, au rang desquels se trouve le milieu cyber.

Intraterre : EN SAVOIR + **Internet : EN SAVOIR +**

Les articles complets sont accessibles sur le site www.penseemiliterre.fr ou directement sur les liens indiqués dans chaque brève.

LES ENGAGEMENTS DANS LE CYBERESPACE

La cyberdéfense est d'abord un combat, par Arnaud Le Dez, chercheur associé au pôle « mutation des conflits » du Centre de recherche des écoles de Saint-Cyr Coëtquidan

Depuis 2013 la cyberdéfense, ce domaine souvent méconnu et qui pourtant ressemble aux conflits armés que nous connaissons, permet ce combat numérique qui est aujourd'hui indispensable si l'on veut aussi dominer dans le cyberespace pour vaincre. Nous avions l'habitude de faire de la sécurité des systèmes d'information. La cyberdéfense est fondamentalement autre chose dans un espace numérique extrêmement vaste. Le combat numérique, nourri par le renseignement qui permet cette nouvelle capacité, se planifie et se conduit en reproduisant une dialectique guerrière entre attaquants et attaqués. Il en va spécifiquement de la différence entre cyberdéfense et cybersécurité comme celle plus générale entre défense et sécurité dans les opérations militaires.

Intraterre : EN SAVOIR + **Internet : EN SAVOIR +**

La conquête des ressources humaines en cyberdéfense, par le commandant Jean-François Caverne, officier stagiaire à l'EMSST (cycle académique 2018-2019)

Si la composante cyberdéfense est aujourd'hui considérée comme un vecteur incontournable du succès des opérations militaires et de la souveraineté nationale, il n'en demeure pas moins que cette composante naissante doit impérativement se consolider et livrer la bataille des ressources humaines. Une piste prometteuse consisterait à fédérer les initiatives et développer une filière militaire de cyberdéfense complète pour accroître l'attractivité et la visibilité d'un domaine en pleine expansion et en quête de ressources rares et très recherchées.

Pour comprendre comment relever ce défi de robustesse et d'efficacité, il faut tout d'abord considérer le jeune modèle choisi par la France. Ensuite, il convient de comprendre que la ressource ne doit pas être réduite à la seule dimension technique, mais s'appuyer sur l'implication de l'ensemble du personnel au bénéfice du projet stratégique. Enfin, la rareté et la volatilité des ressources poussent à regarder vers la capitalisation sur différentes initiatives pour développer une filière stratégique.

Intraterre : EN SAVOIR + **Internet : EN SAVOIR +**

La stratégie française de cyberdéfense, par Aude Géry, chercheur associé au sein de GEODE, centre de recherche et de formation sur la géopolitique de la Datasphère, et officier de réserve à l'EMSST

L'expansion et l'interconnexion des systèmes d'information et de communication ont fait apparaître de nouveaux défis pour les États, tant en termes de développement que de sécurité. Pour y faire face, ces derniers, dont la France, ont adopté différentes stratégies, en fonction de leur histoire, de leur fonctionnement mais également de la façon dont le cyberespace a été appréhendé. La stratégie française de cyberdéfense se distingue par plusieurs caractéristiques, au plan doctrinal et organisationnel, qui lui sont propres. Si ces deux dernières années ont été particulièrement prolifiques au plan doctrinal, on relève une continuité et une cohérence d'action visant à doter la France des moyens d'assurer sa sécurité, et celle de ses citoyens, dans le cyberespace mais également d'y projeter sa puissance.

Intraterre : EN SAVOIR + **Internet : EN SAVOIR +**

Les articles complets sont accessibles sur le site www.penseemiliterre.fr ou directement sur les liens indiqués dans chaque brève.

LES ENGAGEMENTS DANS LE CYBERESPACE

L'organisation de la cyberdéfense au sein de l'OTAN, par le capitaine Frédéric Segonne, officier stagiaire à l'EMSST (cycle académique 2018-2019)

Si la cyberdéfense est, aujourd'hui, au cœur des préoccupations tant au niveau étatique qu'au sein d'organisations internationales, la prise de conscience de l'importance des menaces cybernétiques est relativement récente. A l'image de la majorité de ses pays membres, l'OTAN a dû développer une politique de cyberdéfense et se doter des moyens de la mettre en œuvre. Son objectif initial étant d'assurer la sécurité de ses systèmes d'information, la finalité de cette politique est de permettre à l'Alliance de riposter de manière proportionnée ou de mener des attaques préventives dans le cyberespace. La cyberdéfense a fait son apparition dans les sujets d'attention de l'OTAN à compter du sommet de Prague en 2002, préconisant alors un renforcement des capacités de l'Alliance contre les attaques informatiques. Dans un premier temps, c'est la protection de ses propres systèmes d'information et de communication qui a mobilisé l'Alliance, avec notamment la mise en place de la capacité OTAN d'intervention en cas d'incident informatique. L'OTAN dispose aujourd'hui des capacités lui permettant d'assurer sa résilience face aux cyberattaques qui la visent. L'Alliance continue à les améliorer et à en développer de nouvelles. Cette construction doit se poursuivre tout en faisant face aux nouvelles menaces du cyberespace. La résolution de l'Alliance est, en effet, aussi forte dans le cyberespace que dans chaque milieu où elle a des intérêts. L'OTAN doit maintenant montrer que sa détermination à dissuader toute agression contre ses membres demeure et ne fait finalement que s'étendre à un quatrième domaine opérationnel.

Intraterre : EN SAVOIR + **Internet : EN SAVOIR +**

La conduite des opérations cyber, par le commandant Nicolas Chevrier, du Commandement de la cyber-défense

Depuis 2013, le Livre blanc sur la défense et la sécurité nationale, affirme que le cyberespace est désormais un champ de confrontation à part entière, tandis que notre stratégie est pensée de manière à ce que notre souveraineté nationale puisse s'y exercer et être respectée. Au-delà des mots et de la nature du cyberespace, une réalité bien tangible se fait jour où des États et de puissants groupes assument l'expression de leur territorialité dans ce nouvel espace. Dans ce contexte tumultueux, il devient donc indispensable, pour la France et le ministère des Armées en particulier, de mener des opérations de cyberdéfense.

Ainsi, il est possible d'agir au sein du cyberespace mais aussi depuis le cyberespace à destination des quatre milieux Terre, Air, Mer et Espace. Du point de vue du ministère des Armées, cela revient à mener des opérations de Lutte Informatique Offensive (LIO) et de Lutte Informatique Défensive (LID) dans un cadre légal clair, qui décrit l'emploi de l'arme cyber, partout où les armées sont engagées. A ce propos, le CEMA, dans son discours prononcé en janvier 2019 à l'occasion de la publication par le ministère de sa politique LID et de la doctrine d'emploi de la LIO à des fins militaires, résumait alors l'ensemble du spectre des missions militaires selon le triptyque « renseigner – défendre – agir ». Il ajoutait que les nouveaux moyens de lutte (i.e. cyber) pouvaient dès lors « se combiner et, si nécessaire se substituer aux autres capacités militaires […] ». Ici, il est plus intéressant d'étudier la combinaison des capacités cyber, notamment défensives, en appui d'opérations cinétiques traditionnelles.

Intraterre : EN SAVOIR + **Internet : EN SAVOIR +**

Les articles complets sont accessibles sur le site www.penseemiliterre.fr ou directement sur les liens indiqués dans chaque brève.

LES ENGAGEMENTS DANS LE CYBERESPACE

Les systèmes d'information, l'intelligence artificielle et le cyber, par Mesdames Claire Angelotti et Clarisse Naegels, rédacteurs au pôle études et prospective du CDEC

Depuis les années 2000, les différents textes officiels relatifs à la défense et la sécurité nationales - Livre blanc, Revue stratégique, loi de programmation militaire - mettent l'accent sur la « connaissance et l'anticipation » en tant que fonction stratégique des Armées. Pour assurer cette fonction stratégique, et dans le but de garantir une supériorité opérationnelle des forces françaises, la maîtrise de l'information et l'optimisation des systèmes d'information de défense sont devenues des enjeux majeurs pour les Armées. Le développement de l'intelligence artificielle (IA) modifie aujourd'hui l'utilisation des systèmes d'information et le traitement des données. Souvent décriée comme une vulnérabilité cyber, l'IA est aussi une opportunité dans le domaine de la cybersécurité. Plus performante que l'humain dans le domaine de la détection, l'IA devrait pouvoir assurer une fonction de protection des réseaux. Au travers du programme SCORPION, l'armée de Terre souhaite intégrer cette technologie à ses systèmes d'armes. Compte tenu de son faible niveau de développement actuel, l'intégration de l'IA dans les systèmes d'armes prendra néanmoins du temps ; un temps probablement nécessaire à une meilleure adaptation du matériel et des forces à cette technologie.

Intraterre : EN SAVOIR + **Internet : EN SAVOIR +**

Les câbles sous-marins entre vulnérabilité et enjeu stratégique, par le commandant Hélène Gorbéna, officier stagiaire à l'EMSST (cycle académique 2018-2019)

Les câbles sous-marins tapissent le fond des mers et des océans depuis le XIXe siècle et sont encore méconnus du grand public. Or, contrairement à une idée encore assez répandue, seul 1% du trafic d'Internet transite par les réseaux satellitaires. Les 99% des flux de données restants passent par ces câbles. Depuis la pose du premier câble télégraphique entre la France et l'Angleterre en 1851, leur nombre a augmenté de façon exponentielle. Le site « submarinecablemap.com » recense plus de 430 câbles en 2018 qui transportent données et/ou énergie au moyen de différentes technologies, la fibre optique étant aujourd'hui massivement utilisée pour les télécommunications. Les câbles combinent, en effet, de nombreux avantages comparativement aux satellites : des coûts bien moindre, permettant de proposer des tarifs compétitifs, des débits et qualités de transmission élevés, une durée de vie importante. Or les câbles sous-marins sont un sujet essentiel car les vulnérabilités sont nombreuses et les menaces concrètes. Ils représentent un enjeu critique, les États étant fortement dépendants du bon fonctionnement des réseaux et de l'intégrité des données qui y circulent. Ils sont donc une composante physique qu'il est essentiel de surveiller et de protéger afin d'en limiter les vulnérabilités. À la lumière des luttes d'influence qui se jouent dans le cyberespace, la protection des données sensibles et la souveraineté numérique sont également des enjeux majeurs dont les câbles sous-marins ne représentent qu'un volet.

Intraterre : EN SAVOIR + **Internet : EN SAVOIR +**

«Du cyber et de la guerre» - Fondation pour la recherche stratégique, 12 septembre 2019

Olivier Kempf, chercheur associé à la FRS, analyse l'évolution du rôle du cyber dans et hors de la guerre. Son analyse sémantique des notions reliées au cyber le conduit à préférer l'emploi du terme de cybersécurité à celui de cyberdéfense. Il montre également l'inopérance du terme de cyberguerre, en raison de l'absence de létalité qu'engendre ses attaques et de la diversité des lieux d'expression des conflits. Il lui préfère la notion de cyberconflictualité, qui se traduirait par trois types de cyber agressions : l'espionnage, le sabotage et la subversion. Ensuite, il indique quels sont les trois modes d'action stratégiques dans le cyber : la défense, le renseignement et l'offensive. Enfin il montre comment "le cyberespace permet la mise en place d'une nouvelle conflictualité, qui va, d'une certaine façon, fusionner les champs traditionnels des hostilités : aussi bien les guerres militaires que les oppositions géopolitiques ou les concurrences économiques."

EN SAVOIR +

«L'avenir de la cybersécurité européenne» - Rapport d'information de la Commission des Affaires étrangères de l'Assemblée nationale, 14 novembre 2019

Chaque année, 80% des entreprises européennes connaissent au moins un "incident de cybersécurité". Dans certains États membres de l'Union, 50% des crimes perpétrés interviendraient dans le champ de la cybercriminalité. Dans ce contexte, la Commission des Affaires étrangères de l'Assemblée nationale s'interroge sur l'avenir de la cybersécurité au niveau européen. La France occupe une place importante sur ce terrain en Europe car elle dispose d'une expertise ancienne et reconnue, incarnée notamment par son agence nationale, l'ANSSI. La législation européenne récente (directive SRI et Acte de cybersécurité) est certes venue poser les jalons d'une collaboration européenne efficace sous le patronage d'une agence dédiée : l'ENISA ou AESRI (Agence européenne chargée de la sécurité des réseaux et de l'information). Cependant, l'enjeu de la cybersécurité à l'échelle communautaire recouvre des problématiques de défense à la fois nationales et européennes. À partir des observations recueillies, le rapport de la Commission se propose, dans un premier temps, de présenter les enjeux de la cybersécurité en Europe ces dernières années. Il préconise ensuite la désignation d'une personnalité politique de référence dans chaque État membre, susceptible d'offrir une meilleure visibilité aux enjeux cyber, face à la diversité des instances nationales. Enfin, le rapport examine également les modalités de la certification européenne induites par le nouveau règlement et la mise en oeuvre de l'Acte de cybersécurité afin de faire converger les secteurs public et privé.

EN SAVOIR +

«Qu'est-ce que la puissance numérique ?» - IFRI, novembre 2019

Dans une étude publiée en novembre 2019, Jean-Christophe Noël, chercheur à l'IFRI, analyse l'influence grandissante de la puissance numérique, qu'il définit comme la "capacité d'un acteur à exploiter les flux de données numériques pour contribuer à modifier le comportement d'autres acteurs sur la scène internationale". Nouvelle forme de domination politique, la puissance numérique offrirait la possibilité de contourner les niveaux tactique, opératif et stratégique pour influencer directement la population d'un adversaire sans recourir à la force. Néanmoins, les formes les plus avancées de cette puissance ont un coût financier important et nécessiteront un volontarisme politique pour être mises en œuvre. Si leur avenir dépendra avant tout du développement de nouvelles technologies, l'émergence progressive d'une "identité numérique" impliquera de réguler l'usage des données.

EN SAVOIR +

"Künstliche Intelligenz in Landstreitkräften (Artificial intelligence in land force)", Position paper, Amt für Heeresentwicklung - Bundesheer, octobre 2019

Premier d'une série de trois études consacrées aux évolutions majeures que devraient connaître l'armée de Terre allemande (robotique/système autonome, numérisation et intelligence artificielle), ce document d'orientation présente la position de la Bundesheer en matière d'intelligence artificielle (IA). Partant du constat selon lequel les confits futurs s'articuleront autour de la combinaison de moyens de combat conventionnels et non-conventionnels (cyberattaques, systèmes létaux autonomes) - une approche baptisée Hyperwar - la Bundesheer considère l'IA comme une opportunité permettant de faciliter l'usage de systèmes autonomes et d'améliorer le processus de commandement. Elle reconnaît quatre champs d'action principaux dans lesquels l'IA pourrait apporter une plus-value : l'amélioration des systèmes d'arme existants, la recherche et le développement, la gestion du personnel et des équipements, ainsi que l'entraînement. Enfin, plusieurs recommandations sont émises, parmi lesquelles le recrutement de spécialistes de l'IA, la mise en place d'une agence spécialisée, le renforcement de la coopération entre militaires, chercheurs et industriels, ainsi que la création de bases de données indispensables au *machine learning*.

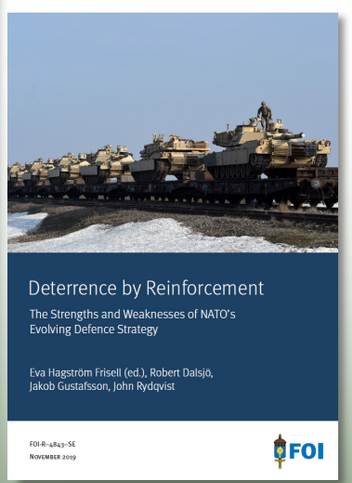
EN SAVOIR +

"AI and Irregular Warfare: An Evolution, Not a Revolution" - War on the Rocks, 31 octobre 2019

L'article se présente comme une réponse aux études mandatées par la Commission de la Sécurité Nationale sur l'intelligence artificielle américaine. Les auteurs ont choisi de traiter la première question de la réflexion : "Comment l'intelligence artificielle affectera-t-elle la nature même de la guerre ?" en focalisant leur attention sur les guerres non-conventionnelles, qui, selon eux, seront les principaux conflits de demain pour les États-Unis. Ils partent du postulat selon lequel l'intelligence artificielle aurait un impact sur les conflits où la suprématie en termes d'information et de compréhension sera décisive avec l'amélioration de la vitesse, de la précision et de l'efficacité induite par les nouvelles technologies. Les conflits non-conventionnels requièrent à la fois une compréhension physique et sociale du milieu. D'après eux, l'intelligence artificielle jouerait un rôle de facilitateur en complément de l'analyse humaine. Néanmoins, les auteurs nuancent cette évolution en insistant notamment sur l'importance de conserver l'humain au coeur du processus et sur le danger que constituerait à terme l'intelligence artificielle (notamment la capacité pour l'ennemi de reconnaître les belligérants adverses via la reconnaissance faciale dans des conflits non-déclarés). Certes l'intelligence artificielle constitue une évolution majeure pour le domaine militaire, mais elle n'est cependant pas une "révolution" technologique à part entière qui bouleverserait fondamentalement le champ de la guerre moderne.

EN SAVOIR +

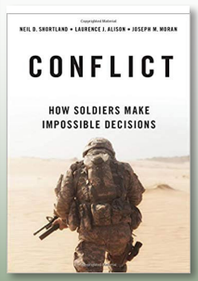
"Deterrence by reinforcement - The strengths and weaknesses of NATO's evolving defence strategy" - FOI [Agence suédoise de recherche pour la défense], 19 novembre 2019



Depuis 2014, la nature des opérations conduites par l'OTAN a évolué. D'opérations de gestion de crises sur des théâtres extérieurs, l'OTAN conduit à présent des opérations de dissuasion et de défense sur les territoires de ses États-membres. L'organisation a fait le choix d'une présence limitée sur le front est de l'Europe, où sa crédibilité repose sur sa capacité à renforcer rapidement cette présence. L'étude souhaite évaluer cette capacité de renforcement en cas d'attaque russe contre les pays baltes. De nombreux obstacles pratiques, juridiques et d'infrastructures, la ralentissent, auxquels l'étude se propose d'apporter des solutions. La question essentielle à laquelle l'OTAN doit répondre est de savoir si elle doit choisir la dissuasion ou se préparer à la défense.

EN SAVOIR +

Conflict: How Soldiers Make Impossible Decisions, Neil D. Shortland, Laurence J. Alison, Joseph M. Moran, Cambridge University Press, 2019, 248 pages

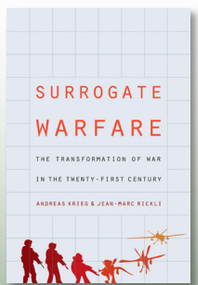


Dans cet ouvrage, trois psychologues tentent de comprendre quel est le processus de prise de décision des militaires en situation difficile. Ils choisissent d'aborder cette question à l'aune du concept d'inertie décisionnelle. Ce concept caractérise l'impossibilité pour un décideur de faire un choix. Les auteurs émettent l'hypothèse que les militaires seraient moins enclins à ce genre de défaillance décisionnelle. Grâce à des entretiens avec des opérationnels qui ont été confrontés à de telles situations, les auteurs confirment leur hypothèse et en explicitent les raisons. Le processus décisionnel propre aux militaires consisterait à prendre la décision qui correspond aux valeurs les plus importantes à leurs yeux, ce qui les prémunirait du risque d'inertie décisionnelle, auquel sont confrontés plus fréquemment les civils. **LC**

Les opérations en essaim : histoire et avenir, chef de bataillon Mathieu Peter, stagiaire de la 25e promotion de l'École de Guerre, 2018, 113 pages

Le chef de bataillon Mathieu Peter présente dans ce mémoire l'apport académique que constitue l'étude des opérations en essaim pour appréhender la guerre moderne. Ce « nouveau paradigme de la guerre » repose sur quatre principes (liberté d'action, convergence-dispersion, incertitude et résilience) et sur deux facteurs de succès (supériorité en renseignement et capacité à délivrer un tir d'arrêt). Pour illustrer sa démonstration, l'auteur analyse huit conflits depuis l'Antiquité jusqu'à nos jours, de la bataille de Carrhes à l'intervention russe en Tchétchénie, en passant par les campagnes napoléoniennes. L'auteur insiste également sur l'omniprésence des opérations en essaim dans les conflits militaires modernes, lesquelles sont de plus en plus employées par des adversaires non-étatiques. Face au défi que représentent les *modus operandi* de ces acteurs et les ruptures technologiques, ce cadre d'analyse permettrait de répondre aux problèmes rencontrés par les forces armées modernes dans l'anticipation de la guerre de demain. **VF**

The Russian Understanding Of War. Blurring the Lines Between War and Peace, Oscar Jonsson, Georgetown University Press, 2019, 187 pages



Les conflits en Crimée et dans le Donbass ont fait naître depuis 2014 une abondante littérature sur la Russie et ses nouvelles formes de conflictualité, au travers du concept de guerre hybride. Pour l'auteur, ces débats importent moins que la façon dont les militaires et les élites russes pensent la guerre dans un environnement international marqué par la compétition entre puissances. Il en tire trois caractéristiques : 1) la pensée militaire russe est un héritage de la pensée soviétique qui voit dans la guerre la continuation de la politique par des moyens militaires, 2) ces moyens traditionnels ne correspondent plus aux nouvelles formes de la guerre qu'autorisent les bouleversements technologiques (NTIC), 3) il convient d'opérer une bascule de l'emploi de moyens militaires vers celui de moyens non-militaires (guerre de l'information et subversion politique). Cet ouvrage nous donne donc les clés d'une meilleure compréhension de la Russie, préalable à toute négociation. **GL**

Atlas militaire et stratégique, Bruno Tertrais, Hugues Piolet, Autrement, 2019, 96 pages

L'Atlas militaire et stratégique, sous la direction de Bruno Tertrais, est original par son approche : il propose d'appréhender les défis stratégiques contemporains en se fondant sur des cartes et des graphiques autour d'une trentaine de fiches thématiques. Si cette édition 2019 s'ouvre sur un constat plutôt optimiste - le nombre de conflits armés entre États se situe à un niveau historiquement bas - la conflictualité, elle, n'en demeure pas moins omniprésente. Cet outil se veut donc un vade-mecum pour comprendre les stratégies des principales puissances (Chine, États-Unis, Russie) en s'appuyant sur des données actualisées et fiables sur l'état des forces en présence dans le monde. De la maîtrise des armements à l'espace extra-atmosphérique, en passant par le cyberespace, la lutte contre le terrorisme et le développement de nouvelles technologiques, cet atlas propose une analyse à la fois détaillée et synthétique, d'un monde sous tension. **GS**